AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims.

1. (CURRENTLY AMENDED) A system comprising: ~~a processor unit for accessing a memory storing instructions therein that when executed by the processor unit intercepts multimedia documents disseminated from a first network, the system comprising~~

a memory;

processor means for intercepting documents from, and having a connection to, a first network;

said processor means storing information relating to said documents in said memory;

said processor means having a module for intercepting and processing packets of information each including an identification header and a data body, the packet interception and processing module ~~comprising a~~ comprising first ~~unit~~ means for intercepting packets disseminated from the first network, ~~a unit~~ means for analyzing the headers of packets in order to determine whether a packet under analysis forms part of a connection that has already been set up, ~~a unit~~ means for processing packets recognized as forming part of a connection that has already been set up to determine the identifier of each received packet and to access a storage container where the data present in each received packet is saved, and ~~a unit~~ means for creating an automaton for processing the received packet belonging to a new connection if the packet header analyzer ~~unit shows~~ means show that a packet under analysis constitutes a request for a new connection, the ~~unit~~ means for creating an automaton comprises ~~a unit~~ means for creating a new storage container for containing the resources needed for storing and managing the data produced by the ~~unit~~ means for processing packets associated with the new connection, a triplet comprising <identifier, connection state flag, storage container> being created and being associated with each connection by said ~~unit~~ means for creating an automaton, and said system further comprising ~~a unit~~ means for analyzing the content of data stored in the containers, for recognizing the protocol used from a set of standard protocols such as http, SMTP, FTP, POP, IMAP, TELNET, P2P, for analyzing the content transported by the protocol, and for reconstituting the intercepted documents.

2. (CURRENTLY AMENDED) The system according to claim 1, wherein the analyzer ~~unit~~ means and the processor ~~unit~~ means comprise a first table for setting up a connection and containing for each connection being set up an identifier "connectionId" and a flag "connectionState", and a

second table for identifying containers and containing, for each connection that has already been set up, an identifier "connectionId" and a reference "containerRef" identifying the container dedicated to storing the data extracted from the frames of the connection having the identifier "connectionId".

3. (PREVIOUSLY PRESENTED) The system according to claim 2, wherein the flag "connectionState" of the first table for setting up connections can take three possible values depending on whether the detected packet corresponds to a connection request made by a client, to a response made by a server, or to a confirmation made by the client.

4. (CURRENTLY AMENDED) The system according to claim 1, wherein the first packet interception ~~unit~~means, the packet header analyzer ~~unit~~means, the automaton creator ~~unit~~means, the packet processor ~~unit~~means, and the ~~unit~~means for analyzing the content of data stored in the containers operate in an independent and asynchronous manner.

5. (PREVIOUSLY PRESENTED) The system according to claim 1, further comprising a first storing module for storing the content of documents intercepted by the module for intercepting and processing packets, and a second storing module for storing information relating to at least the sender and the destination of intercepted documents.

6. (PREVIOUSLY PRESENTED) The system according to claim 5, further comprising a third storing module for storing information relating to the components that result from detecting the content of intercepted documents.

7. (CURRENTLY AMENDED) A system comprising; ~~a processor unit for accessing a memory storing instructions therein that when executed by the processor unit intercept:~~

a memory;

processor means for intercepting multimedia documents disseminated from, and having a connection to, a first network~~, the system comprising~~;

said processor means storing information relating to said documents in said memory;

said processor means having a module for intercepting and processing packets of information each including an identification header and a data body, the packet interception and processing module comprising ~~a first unit~~ first means for intercepting packets disseminated from the first network, ~~a unit~~means for analyzing the headers of packets in order to determine whether a packet under analysis forms part of a connection that has already been set up, ~~a unit~~means for processing packets recognized as forming part of a connection that has already been set up to determine the identifier of each received packet and to access a storage container where the data present in each received packet is saved, and ~~a unit~~means for creating an automaton for processing the received packet belonging to a new connection if the packet header analyzer ~~unit~~means shows that a packet under analysis constitutes a request for a new connection, the ~~unit~~means for creating an automaton comprising ~~a unit~~means for creating a new storage container for containing the resources needed for storing and managing the data produced by the ~~unit~~means for processing packets associated with the new connection, a triplet comprising <identifier, connection state flag, storage container> being created and being associated with each connection by said ~~unit~~means for creating an automaton, and said system further comprising ~~a unit~~means for analyzing the content of data stored in the containers, for recognizing the protocol used from a set of standard protocols such as in particular http, SMTP, FTP, POP, IMAP, TELNET, P2P, for analyzing the content transported by the protocol, and for reconstituting the intercepted documents, the system further comprising a centralized system comprising ~~a unit~~means for producing fingerprints of sensitive documents under surveillance, ~~a unit~~means for producing fingerprints of intercepted documents, ~~a unit~~means for storing fingerprints produced from sensitive documents under surveillance, ~~a unit~~means for storing fingerprints produced from intercepted documents, ~~a unit~~means for comparing fingerprints coming from the ~~unit~~means for storing fingerprints produced from intercepted documents with fingerprints coming from the ~~unit~~means for storing fingerprints produced from sensitive documents under surveillance, and ~~a unit~~means for processing alerts, containing the references of intercepted documents that correspond to sensitive documents.

8. (CURRENTLY AMENDED) The system according to claim 7, further comprising a selector ~~unit~~means responding to the ~~unit~~means for processing alerts to block intercepted documents or to

forward them towards a second network, depending on the results delivered by the ~~unit~~means for processing alerts.

9. (CURRENTLY AMENDED) The system according to claim 7, wherein the centralized system further comprises ~~a unit~~means for associating rights with each sensitive document under surveillance rights, and ~~a unit~~means for storing information relating to said rights, which rights define the conditions under which the document can be used.

10. (PREVIOUSLY PRESENTED) The system according to claim 1, interposed between a first network of the LAN type and a second network of the LAN type.

11. (PREVIOUSLY PRESENTED) The system according to claim 1, interposed between a first network of the Internet type and a second network of the Internet type.

12. (PREVIOUSLY PRESENTED) The system according to claim 1, interposed between a first network of the LAN type and a second network of the Internet type.

13. (PREVIOUSLY PRESENTED) The system according to claim 1, interposed between a first network of the Internet type and a second network of the LAN type.

14. (PREVIOUSLY PRESENTED) The system according to claim 13, further comprising a generator for generating requests from sensitive documents to be protected, in order to inject requests into the first network.

15. (CURRENTLY AMENDED) The system according to claim 14, wherein the request generator comprises:

~~a unit~~means for producing requests from sensitive documents under surveillance;

~~a unit~~means for storing the requests produced;

~~a unit~~means for mining the first network with the help of at least one search engine using the previously stored requests;

~~a unit~~means for storing the references of suspect files coming from the first network; and

~~a unit~~means for sweeping up suspect files referenced in the ~~unit~~means for storing references and for sweeping up files from the neighborhood, if any, of the suspect files.

16. (CURRENTLY AMENDED) The system according to claim 7, wherein said ~~unit~~means for comparing fingerprints deliver a list of retained suspect documents having a degree of pertinence relative to sensitive documents, and the alert processor ~~unit~~means delivers the references of an intercepted document when the degree of pertinence of said document is greater than a predetermined threshold.

17. (CURRENTLY AMENDED) The system according to claim 7, further comprising, between said ~~unit~~means for comparing fingerprints and said ~~unit~~means for processing alerts, a calculating module for calculating the similarity between documents, which calculating module comprises:

a) ~~a unit~~means for producing an interference wave representing the result of pairing between a concept vector taken in a given order defining the fingerprint of a sensitive document and a concept vector taken in a given order defining the fingerprint of a suspect intercepted document; and

b) ~~a unit~~means for producing an interference vector from said interference wave enabling a resemblance score to be determined between the sensitive document and the suspect intercepted document under consideration, the ~~unit~~means for processing alerts delivering the references of a suspect intercepted document when the value of the resemblance score for said document is greater than a predetermined threshold.

18. (CURRENTLY AMENDED) The system according to claim 7, further comprising, between said ~~unit~~means for comparing fingerprints and said ~~unit~~means for processing alerts, a calculating module for calculating similarity between documents, which calculating module comprises a ~~unit~~means for producing a correlation vector representative of the degree of correlation between a concept vector taken in a given order defining the fingerprint of a sensitive document and a concept

vector taken in a given order defining the fingerprint of a suspect intercepted document, the correlation vector enabling a resemblance score to be determined between the sensitive document and the suspect intercepted document under consideration, the ~~unit~~means for processing alerts delivering the references of a suspect intercepted document when the value of the resemblance score for said document is greater than a predetermined threshold.

19. (CURRENTLY AMENDED) A system comprising: ~~a processor unit for accessing a memory storing instructions therein that when executed by the processor unit intercepts~~

a memory;

processor means for intercepting documents disseminated from, and having a connection to, a first network~~, the system~~;

said processor means storing information relating to said documents in said memory;

said processor means having ~~comprising~~ a module for intercepting and processing packets of information each including an identification header and a data body, the packet interception and processing module comprising ~~a first unit~~ first means for intercepting packets disseminated from the first network, ~~a unit~~means for analyzing the headers of packets in order to determine whether a packet under analysis forms part of a connection that has already been set up, ~~a unit~~means for processing packets recognized as forming part of a connection that has already been set up to determine the identifier of each received packet and to access a storage container where the data present in each received packet is saved, and ~~a unit~~means for creating an automaton for processing the received packet belonging to a new connection if the packet header analyzer ~~unit~~means shows that a packet under analysis constitutes a request for a new connection, the ~~unit~~means for creating an automaton comprising ~~a unit~~means for creating a new storage container for containing the resources needed for storing and managing the data produced by the ~~unit~~means for processing packets associated with the new connection, a triplet comprising <identifier, connection state flag, storage container> being created and being associated with each connection by said ~~unit~~means for creating an automaton, and the system further comprising ~~a unit~~means for analyzing the content of data stored in the containers, for recognizing the protocol used from a set of standard protocols such as http, SMTP, FTP, POP, IMAP, TELNET, P2P, for analyzing the content transported by the protocol, and for reconstituting the

intercepted documents, wherein the first packet interception ~~unit~~means, the packet header analyzer ~~unit~~means, the automaton creator ~~unit~~means, the packet processor ~~unit~~means, and the ~~unit~~means for analyzing the content of data stored in the containers operate in an independent and asynchronous manner, and wherein the system further comprises a first storing module for storing the content of documents intercepted by the module for intercepting and processing packets, and a second storing module for storing information relating to at least the sender and the destination of intercepted documents.